What is claimed is:

1. A virtual network communication system for effecting secure communications between user agents at different sites within said virtual network, comprising:

at least one Private Tuple Space within each of said sites for effecting intra-site communications between agents at each of said sites;

a Shared Tuple Space for effecting inter-site communications between said different sites; and

a Coordinator Manager within each of said sites for receiving user initiated communication requests from said Private Tuple Space to communicate between user agents at said different sites, authenticating said requests and in response dynamically creating and managing instances of Coordinators at each of said different sites which embed messages from said user agents in secure tuples and exchange said secure tuples over said Shared Tuple Space.

2. The virtual network communication system of claim 1, wherein each said Coordination Manager further includes an Authentication Agent for negotiating authentication and key exchange protocols there between and in response generating and forwarding an inner key to each of said user agents at said different sites for encrypting and decrypting said messages embedded in said secure tuples, and for generating two dynamic identifiers used to create said Coordinator instances and a hashed value of said inner key for encrypting and decrypting said secure tuples.

3. The virtual network communication system of claim 2, further including a Data Repository within each of said sites for storing authentication data applicable to local ones of said user agents, said authentication data being accessible to said Authentication Agent for negotiating said authentication and key exchange protocols.

4. The virtual network communication system of claim 1, wherein said Coordinator Manager further includes a dynamic table containing IDs of all active

ones of said user agents and corresponding ones of said Coordinators for detection of impersonation attacks against said virtual network communication system.

5. The virtual network communication system of claim 1, wherein said Coordinators calculate and verify digital signatures for each of said secure tuples thereby ensuring message integrity.

6. A method of effecting secure virtual network communications between user agents at different sites within said virtual network, comprising the steps of:

authenticating user initiated requests to communicate between user agents at said different sites;

generating and forwarding an inner key to each of said user agents at said different sites for encrypting and decrypting messages exchanged there between; and

dynamically creating and managing instances of Coordinators at each of said different sites for embedding said messages in secure tuples and exchanging said secure tuples over a Shared Tuple Space between said different sites.

7. The method of claim 6, further comprising the steps of generating two dynamic identifiers for creating said Coordinator instances and generating a hashed value of said inner key as said outer key for encrypting and decrypting said control information in said secure tuples.

8. The method of claim 6, further comprising the step of separating QoS and other control information needed by said network from user information communicated between said user agents.

9. The method of claim 8, further comprising the steps of:

encrypting and decrypting said user information in embedded tuples exchanged on Shared Tuple Space by each of said user agents at said different sites using said inner key; and

encrypting and decrypting said secure tuples and control information exchanged on said Shared Tuple Space by said Coordinator instances using a hash value of said inner key for effecting secure dynamic sessions.